Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.5, No.1, 2015
www.iiste.org

On Applications of Transitive Permutation Groups To Wreath Product

*Apine, E.
Department of Mathematics, University of Jos, PMB 2084, Jos, Nigeria
* e-mail of the corresponding author: : apineen@gmail.com

Abstract

In this article we investigate and examine some of our results from transitive permutation groups which have some bearing to wreath product

Keywords: transitive, permutation, group, wreath product

I. INTRODUCTION

Here we prove some properties of transitive groups that bear consequences upon the Wreath Product of two permutation groups.

II. RESULTS

1.1 Lemma

Let $C \leq Sym$ (n), then C acts transitively on a set Δ if and only if C is cyclic, where
$|\Delta| \leq n$.

Proof

Suppose C acts transitively on the set $\Delta = \{1, 2, \ldots, r\}$ and $|C| = m$. Let $\alpha \in C$, $\alpha \neq (1)$, then $\alpha^s = (1)$ for some positive integer s and by Lagrange's theorem $s|m$. If $s < m$, then some elements of Δ are fixed by α. Consequently C moves elements of a proper subset of Δ, contrary to assumption that C acts transitively on Δ. Thus s = m and C is cyclic generated by α.

Conversely suppose C is cyclic, say $C = \{(1), \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$, where $\alpha^m = (1)$,

Then $r \leq m$ and $\alpha = (1, 2, 3, \ldots, m)$. We observe that for each j (j = 1, 2, . . . , r),

$\alpha^i(j) \equiv i + j \pmod m$, i = 0, 1, 2, … , m – 1. Here $\alpha^0(j) = (1)$ denotes the identity permutation. Clearly for each $i \neq 0$, $i + j \neq j$ and $\alpha^i(j) \in \Delta$. Thus $\alpha^i(j) = k$, for some

$j, k \in \Delta$ and $\alpha^i \in C$. This shows that C is transitive on Δ as required

1.2 Lemma

Let $G \leq Sym$ (n) and $|G| = m$. Then G is the unique permutation group acting on a set Δ with $|\Delta| = r$ if and only if r = m.

Proof

Suppose G is the unique permutation group acting transitively on Δ, then $r|m$ otherwise G will not be transitive on Δ by [1].

If r < m, consider the permutation $\alpha = (r, r-1, \ldots, 1)$ and let $H = \{(1), \alpha, \ldots, \alpha^{r-1}\}$, with $\alpha^r = (1)$. Since for each i (i = 1, 2, …, r -1), we have

Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.5, No.1, 2015

$$\alpha^{i}(j) \equiv \begin{cases} r - i + j(\bmod r) & if\ i \neq 0, \\ j & if\ i = 0 \end{cases}$$

holds for j = 1, 2, . . . , r and r - i + j ≠ j for i ≠ 0, it follows that H is transitive on Δ, contradicting the uniqueness of C as the only transitive group acting on Δ, hence r = m.

Conversely if $C^{/}$ is another permutation group acting transitively on Δ with $|\Delta| = r = m$, let $|C^{/}| = n$, then by Lemma 1.1, $G^{/}$ is cyclic and let $C^{/} = \{(1), \beta, \beta^2, \dots, \beta^{n-1}\}$ where

$\beta^n = (1)$. As $C^{/}$ acts transitively on Δ, $\beta^r = (1)$.

Thus $r \leq n$ (1.21)

But n being the order of β means that n ≤ r (1.2.2)

Hence from (1.2.1) and (1.2.2), we see that n = r = m and so $C \cong C^{/}$.

1.3 Proposition

Let G ≤ *Sym* (n), (n > 1) be a permutation group of exponent n such that for 1 ≤ k < n,

$|G|$ = kn. Then G is transitive on the set Ω with $|\Omega|$ = n.

Proof

If k = 1, then $|G|$ = n and as G is of exponent n, G is cyclic. Let α ∈G with

G = < α >, α^n = 1. Then G is transitive on the set Ω = {1, 2, … , n }.

If 1< k < n, as $|G|$ = kn and G is of exponent n, G contains an element a, say of order n. Let H = < a > with a^n =1, then the normalizer of H in G, $N_G(H)$ is of order multiple >1 of n and a divisor of kn, thus $|N_G(H)|$ = kn $= |G|$ and H⊴ G. Let b ∈G – H such that

b^k = (1) and set K= < b >, then H ∩ K= {1} and G = HK. As H◁ G, $b^{-1}ab$ ∈H= <a >, we obtain G = < a, b: a^n =1, b^k = 1, b a = a^r b for some r such that 0 < r < n , a group which contains a cyclic subgroup of order n that is a transitive subgroup of order n and by [1], G is transitive on Ω ={1, 2, … , n } as required.

1.4 Proposition

Let C and D be transitive permutation groups on sets Γ and Δ respectively such that $|\Delta| = |D|$ and $|C| < |D|$, then the wreath product of C and D, W = C wr D with base group P = C^{Δ} is the unique group acting transitively on the set Γ x Δ.

Proof

Let $C^{/}$ and $D^{/}$ be other permutation groups acting transitively on the sets Γ and Δ respectively with $|\Delta| = |D^{/}|$ and consider $W^{/} = C^{/}$ wr $D^{/}$ with base group P = $C^{/\,\Delta}$, then $|W^{/}| = |C^{/}|^{|\Delta|}|D^{/}|$. Since $|\Delta| = |D|$ and $|\Delta| = |D^{/}|$, then $|D| = |D^{/}|$, also by

Lemma 1.1, D and $D^{/}$ are cyclic and so $D \cong D^{/}$. Also since $|P| = |C^{/}|^{|\Delta|} = |C|^{|\Delta|}$ then $|C^{/}| = |C|$ and again by Lemma 1.1, C and $C^{/}$ are cyclic, thus $C \cong C^{/}$. Hence

$|W^{/}| = |C^{/}|^{|\Delta|}|D^{/}| = |C|^{|\Delta|}|D| = |W|$, and so $W \cong W^{/}$.

1.5 Proposition

Let Ω be a set of size *p*, *p* a prime. If G is Sylow *q* – subgroup of *Sym* (Ω), where *q* is a prime with *p* ≠ *q*, then G is not transitive on Ω.

Proof

Suppose G acts transitively on the set Ω, and let $|G| = q^r$, q^r the highest power of *q* dividing p!. As *q* ≠ *p*, we may assume *q* < *p*. Since G is transitive on Ω, G contains at least one element of order *p*, say a. Let H = < a >, with a^p = (1), then $|H|$ = p and by Lagrange's theorem, $p \mid q^r$ which is impossible since *p* and *q* are prime and *q*

$< p$. Hence G is not transitive on Ω.

1.6 Proposition

Let C be a permutation group acting transitively on a set Γ and let $D \leq Sym$ (n) be a cyclic permutation group acting transitively on a set Δ such that $|D| = n$, $|\Delta| = r$, then there exists a unique Wreath Product of C and D, W = C wr D if and only if n = r.

Proof

Suppose $n \neq r$, then $n > r$ (by [1]), let $\Delta = \{1, 2, \dots, r\}$ and consider the base group $P = C^{\Delta} = \{f_i : \Delta \to C,\ i = 1, 2, \dots, |C|^{|\Delta|}\}$. Since D is cyclic, we consider the element $d = (1, 2, 3, 4, \dots, r, r + 1, \dots, n)$ of D, then for $(\alpha, r) \in \Gamma \times \Delta$ and

$i, j \in \{1, 2, \dots, |C|^{|\Delta|}\}$, we have

$(\alpha, r)(f_i d)(f_j d) = (\alpha f_i(r) f_j(rd), d^2) = (\alpha f_i(r) f_j(r + 1), d^2)$ is not defined since

$r + 1 \notin \Delta$, thus W = C wr D does not exist.

Also if $n < r$, consider the generator $\alpha = (1, 2, 3, \dots, n)$ of the cyclic group D. Then

$2, r \in \Delta$, but we cannot find $\alpha^i \in D$ (for any $i \in \{1, 2, 3, \dots, n - 1\}$) such that $\alpha^i(r) = 2$ since $n > r$. This means that D is not transitive on Δ, thus W = C wr D exist implies n = r.

Conversely if n = r, then the elements of the base group

$P = C^{\Delta} = \{f_i: \Delta \to C, i = 1, 2, \dots, |C|^{|\Delta|}\}$ and the elements of $D = < \alpha >$,

$\alpha = (1, 2, 3, \dots, n)$ are all defined and the groups $P = C^{\Delta}$ and D are finite, so is

$|C|^{|\Delta|}|D| = |W|$, hence, W = C wr D is a Wreath Product of C and D. The uniqueness of W = C wr D follows from the fact that any two cyclic groups of the order are isomorphic.

1.7 Lemma

Let C acts transitively on a group Γ and $D \leq Sym$ (n) acting transitively on a set Δ, such that D is not cyclic, $|D| = n$ and $|\Delta| = r$. Then there exists a Wreath product if and only $r|n$, $r \neq n$.

Proof

Let W = C wr D, be a Wreath product of C and D, then $|W|=|C|^{|\Delta|}\ |D|=|C|^r n$. Since D is not cyclic, D contains no elements of order n. Let $\alpha \in D$ such that $\alpha^m = (1)$, then $m|n$. For transitivity of D on Δ, we must have $m = r$, thus and $r \neq n$ and $r|n$.

Conversely if $r \neq n$ and $r|n$, then the cyclic group H generated by the element

$\alpha = (1, 2, \dots, r)$ of D is a subgroup of D transitive on the set $\Delta = \{1, 2, 3, \dots, r\}$. Thus $|H| = r = |\Delta|$ and so by Proposition 1.6, a Wreath product of C and H, W = C wr H exists and is unique.

1.8 Lemma

Let C be a transitive permutation groups on the set Γ and let D and $D^{/}$ be transitive permutation groups on the set Δ. Then the Wreath products W = C wr D and

$W^{/} = C$ wr $D^{/}$ are isomorphic if and only if D and $D^{/}$ are isomorphic.

Proof

If D and $D^{/}$ are not isomorphic, then $|D| \neq |D^{/}|$, hence

$|W|=|C|^{|\Delta|}\ |D| \neq |C|^{|\Delta|}\ |D^{/}| = |W^{/}|$, W and $W^{/}$ do not have the same order and hence cannot be isomorphic.

Conversely if W and $W^{/}$ are not isomorphic then $|W| \neq |W^{/}|$, that is,

$|C|^{|\Delta|}\ |D| \neq |C|^{|\Delta|}\ |D^{/}|$, hence $|D| \neq |D^{/}|$ and so D is not isomorphic to $D^{/}$.

1.9 Theorem

For every prime number p, there is a non – abelian transitive p – group of degree p^2 isomorphic to a unique

Wreath product W = C wr D transitive on the set $\Gamma \times \Delta$ with
$|\Gamma \times \Delta| = p^2$, where $|C| = |\Gamma| = p$, $|D| = |\Delta| = p$.

Proof

Let G be a p – group acting transitively on a set Ω with $|\Omega| = p^2$, p an arbitrary but fixed prime. Then the size of any of its orbits is of cardinality $p^2 > 1$ and it is readily seen that the order of G is at most p^{p+1}. Consequently G is non – abelian and

$|G| = p^{p+1} = p^p p = |C|^{|\Delta|}|D| = |C \text{ wr } D|$. Clearly C and D are cyclic and by Proposition 1.6, the Wreath product C wr D is the unique group acting transitively on set $\Gamma \times \Delta$, of size p^2. Since Wreath products are non – abelian, it follows that $G \cong C$ wr D.

From Theorem 1.9, we deduce the following:

1.10 Corollary

There is, up to isomorphism, only one non – abelian transitive p – group of degree p^2 and order p^{p+1}, namely the Wreath product C_p wr C_p, for every prime number p.

1.11 Corollary

Every transitive p – group of degree p^2 and order p^{p+1} is isomorphic to a unique transitive p – group of degree p^3.

Proof:

We consider the transitive p – group $G^/$ of degree p^3 and order $|G^/| = p^{p+1} = |G|$, where G is transitive p – group of degree p^2. Then by Corollary 1.10, such group G is unique and whence $G^/ \cong G$.

1.12 Remark

We draw our attention here to the fact that a similar result to Corollary 1.10 was obtained by Audu, M. S. in [8].

REFERENCES

[1] Apine, E. and Jelten B.N (2014) Trends in Transitive $p-$Groups and Their Defining Relations. Journal of Mathematical Theory and Modeling, (IISTE). Vol.4. No.11 2014 (192-209).

[2] Apine, E. (2014a) Minimum Size of Generating Set for Transitive p-Group G of degree p^3. International Journal of Mathematics and Statistics Invention (IJMSI) Vol.2(10), 1-4.

[3] Apine, E. (2014b) The number of Transitive p-Groups of Degree p^3. International Journal of Mathematics and Statistics Invention (IJMSI). Vol2(10), (16-18).

[4]. Audu, M. S. (1986) Generating Sets for Transitive Permutation Groups of Prime-Power Order. Abacus Vol. 17 (2): 22-26.

[5] Apine, E; Jelten, B.N.; Homti, E. N.(2015) Transitive 5-Groups of Degree 25 Research Journal of Mathematics and Statistics, Maxwell Scientific Organization- To appear.

[6] Audu. M. S. (1988a) The Structure of the Permutation Modules for Transitive p-groups of degree p^2. Journal of Algebra Vol. 117:227-239.

[7] Audu .M.S. (1988b) The Structure of the Permutation Modules for Transitive Abelian Groups of Prime-Power Order. Nigerian Journal of Mathematics and Applications.Vol.1:1-8.

[8] Audu. M. S. (1988c) The Number of Transitive p-Groups of degree p^2. Advances Modelling and Simulation Enterprises Review. Vol.7(4)9-13.

[9] Audu. M. S. (1989a) Groups of Prime-Power Order Acting on Modules over a Modular Field. . Advances Modelling and Simulation Enterprises Review. Vol.9(4)1-10.

[10] Audu. M. S. (1989b) Theorems About p-Groups. Advances Modelling and Simulation Enterprises Review. Vol.9(4)11-24.

[11] Audu. M. S.(1991a) The Loewy Series Associated with Transitive p-Groups of degree p^2. Abacus. Vol. 2 (2): 1-9.

[12] Audu. M. S. (1991b) On Transitive Permutation Groups. Afrika Mathmatika Journal of African Mathematical Union. Vol. 4 (2): 155-160.

[13]. Audu, M. S. and Momoh, S. U (1993) An Upper Bound for the Minimum Size of Generating Set for a Permutation Group. Nigerian Journal of Mathematics and Applications. Vol. 6: 9-20.

[14]Audu. .M. S, Afolabi. A, and Apine .E (2006) Transitive 3-Groups of Degree $3^n\left(n=2,3\right)$ Kragujevac Journal Mathematics 29 (2006) 71-89.

[15]. Apine, E. (2002). On Transitive p-Groups of Degree at most p^3. Ph.D. Thesis, University of Jos, Jos.

[16]. Cameron, P. J. (1990) Oligomorphic Permutation Groups. Cambridge University Press, Cambridge, 159p.

[17]. Dixon, J. D. (1996) Permutation Groups. Springer – Verlag, New York, 341p.

[18]. Durbin, J. R. (1979) Modern Algebra. John Wiley and Sons Inc., New York, 329p

[19]. Fraleigh, J. B. (1966) A First Course in Abstract Algebra. Addison-Wesley Publishing Company, Reading, 455p.

[20]. Gorenstein, D. (1985) Finite Simple Groups: An Introduction to their Classification. Plenum Press, New-York, 333p.

[21]. Hartley, B. and Hawkes, T. O. (1970) Rings, Modules and Linear Algebra. Chapman and Hall, London, 210p.

[22]. Janus, G. J (1970) Faithful Representation of p-Groups at Characteristic p. Journal of Algebra. Vol. 1: 335-351.

[23]. Kuku, A. O. (1980) Abstract Algebra. Ibadan University Press. Ibadan 419p.

[24] Marshall, H. Jr (1976) The Theory of Groups. Chelsea Publishing Company New York. Second Edition 433p.

[25]. Neumann, P. M. (1976) The Structure of Finitary Permutation Groups. Archiv dev Mathematik (basel). Vol. 27 (1):3-17.

[26]. Pandaraparambil, X. J. (1996) On the Wreath Product of Groups. Ph. D Thesis. University of Ilorin, Ilorin.

[27]. Passman, D. (1968) Permutation Groups. W. A. Benjamin, Inc.,310p.

[28]. Shapiro, L. (1975) Introduction to Abstract Algebra. McGraw-Hill, Inc., New York, 340p.

[29]. Wielandt, H. (1964) Finite Permutation Groups. Academic Press Inc., 113p.

[30] Wielandt,H. (1969) Permutation Groups Through Invariant Relations and Invariant Functions. Lecture Notes, Ohio State University, Columbus, Ohio.